Мораараш Артем Володимирович, магістр*
Яковлєва Інна Дмитрівна, кандидат технічних наук, доцент*
**Чернівецький національний університет*
імені Юрія Федьковича, Чернівці

ШИФРУВАННЯ ТА РОЗШИФРУВАННЯ ДАНИХ ЗА ДОПОМОГОЮ ХЕШ-ФУНКЦІЇ XXHASH

Актуальність використання хеш-функцій у шифруванні та розшифруванні даних обумовлена зростанням обсягів інформації та підвищеними вимогами до її безпеки. У цифрову епоху хеш-функції відіграють ключову роль у забезпеченні конфіденційності, цілісності та автентичності даних. Вони дозволяють ефективно перетворювати великі обсяги інформації на короткі хеш-значення, які використовуються для перевірки цілісності, цифрових підписів і автентифікації.

Мета роботи – розробка та дослідження методів шифрування та розшифрування даних за допомогою хеш-функції xxHash для забезпечення захисту інформації, зокрема перевірки її цілісності, автентифікації та зменшення ризиків компрометації даних у процесі їх зберігання і передачі.

Встановлена мета обумовлює наступні завдання – проведення аналізу аналогів, визначення архітектури алгоритму, обґрунтування та вибір засобів реалізації, проведення тестування, аналіз отриманих результатів, реалізація програмного продукту.

Об’єктом дослідження являються алгоритми для захисту та обробки даних.

Предметом дослідження є застосування хеш-функції xxHash для шифрування та розшифрування даних.

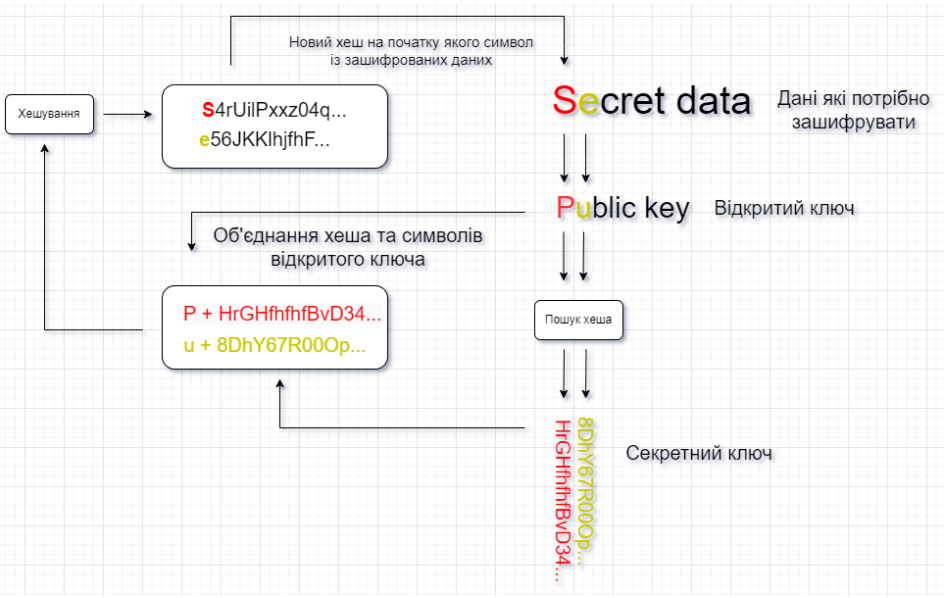

Рисунок 1 – Схема роботи алгоритму

Назва алгоритму	**Попереднє стиснення даних (тільки для HashCipher)**	**Час, сек**	**Пропускна здатність, Мб/сек**	**Розмір даних, МБ**
HashCipher	немає	1.06	4.95	5.25
HashCipher	є	0.0067	771.63	5.25
AES	немає	0.0058	904.23	5.25
DES	немає	0.0484	108.36	5.25

Рисунок 2 – шифрування

Назва алгоритму	**Попереднє стиснення даних (тільки для HashCipher)**	**Час, сек**	**Пропускна здатність, Мб/сек**	**Розмір даних, МБ**
HashCipher	немає	2.08	5.04	10.49
HashCipher	є	0.01	4.38	0.043
AES	немає	0.007	721.50	5.25
DES	немає	0.044	118.62	5.25

Рисунок 3 – розшифрування

Висновки

1. Хеш-функції, зокрема xxHash можна успішно застосовувати для шифрування і розшифрування даних
2. Швидкість алгоритму є прийнятною для невисокопродуктивних задач
3. Ефективність розробленого алгоритму сильно залежить від можливості стиснення вхідних даних
4. Основний недолік розробленого алгоритму це великий розмір ключів
5. Головна перевага такого методу шифрування це значно більша кількість варіантів перебору ключів

Література

1. Алгоритм хешування xxHash. URL: https://xxhash.com/doc/v0.8.2/index.html
2. Алгоритм шифрування AES. URL: https://uk.wikipedia.org/wiki/Advanced_Encryption_Standard
3. Алгоритм шифрування DES.URL: https://uk.wikipedia.org/wiki/Data_Encryption_Standard